

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

19-cv-6032

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

RONNIE KAUFMAN, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Broward County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)
Jonathan Shub, KOHN, SWIFT & GRAF, P.C., 1600 Market St., Suite 2500, Philadelphia, PA 19103, tel: 215-238-1700

DEFENDANTS

WAWA, Inc.

County of Residence of First Listed Defendant Delaware County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question (U.S. Government Not a Party)
- ☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business in This State | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business in Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input checked="" type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District (Specify)
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
28 U.S.C. § 1332 (d) - Diversity of Citizenship

Brief description of cause:

DATA BREACH: NEGLIGENCE, NEGLIGENCE PER SE, DECLARATORY JUDGMENT, CONSUMER FRAUD

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND:

☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DEC 20 2019

DATE
12/20/2019

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

JHS

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

19

6032

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 9397 N.W. 62nd Ct, Parkland, FL 33067Address of Defendant: Wawa, Inc. 260 West Baltimore Pike, Wawa, PA 19063Place of Accident, Incident or Transaction: Several States, including PA and FL

RELATED CASE, IF ANY:

Case Number: _____ Judge: _____ Date Terminated: _____

Civil cases are deemed related when Yes is answered to any of the following questions:

- | | | |
|--|------------------------------|-----------------------------|
| 1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

I certify that, to my knowledge, the within case ☐ is / ☒ is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: _____

Must sign here

Attorney-at-Law / Pro Se Plaintiff

Attorney I.D. # (if applicable)

CIVIL: (Place a ✓ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Patent
- ☐ 6. Labor-Management Relations
- ☐ 7. Civil Rights
- ☐ 8. Habeas Corpus
- ☐ 9. Securities Act(s) Cases
- ☐ 10. Social Security Review Cases
- ☐ 11. All other Federal Question Cases
(Please specify): _____

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury (Please specify): _____
- ☐ 7. Products Liability
- ☐ 8. Products Liability - Asbestos
- ☒ 9. All other Diversity Cases
(Please specify): Negligence - Data Breach

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Jonathan Shub, counsel of record or pro se plaintiff, do hereby certify:

Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of \$150,000.00 exclusive of interest and costs:



Relief other than monetary damages is sought.

DATE: 12/20/2019

Sign here if applicable

Attorney-at-Law / Pro Se Plaintiff

53965 DEC 20 2019

Attorney I.D. # (if applicable)

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

JHS

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

CASE MANAGEMENT TRACK DESIGNATION FORM

Ronnie Kaufman, et al.
Plaintiff

v.

WAWA, Inc. Defendant

CIVIL ACTION

NO. **19** **6032**

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

- (a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ()
- (b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ()
- (c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ()
- (d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ()
- (e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) ()
- (f) Standard Management – Cases that do not fall into any one of the other tracks. ()

12/20/2019
Date

JHS
Attorney-at-law

Plaintiff
Attorney for

215-238-1700

215-238-1968

jshub@kohnswift.com

Telephone

FAX Number

E-Mail Address

DEC 20 2019

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

RONNIE KAUFMAN, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

WAWA, Inc.

Defendant.

19

6032

Civil Action No. _____

Class Action Complaint

Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff Ronnie Kaufman (hereinafter, "Plaintiff"), individually and on behalf of the Class defined below, alleges the following against Wawa, Inc. ("Wawa" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THIS CASE

1. Plaintiff brings this class action case against Defendant Wawa for its major failures to secure and safeguard consumers' personally identifiable information ("PII") which Wawa collected from various sources in connection with the operation of its business as a consumer credit reporting agency, and for failing to provide timely, accurate and adequate notice to Consumer Plaintiff and other Class members that their PII had been stolen and precisely what types of information were stolen.

2. Wawa has acknowledged that a cybersecurity incident ("Data Breach") affecting most of its stores' systems throughout the country. Wawa has not yet disclosed how many U.S.

consumers have been affected by this massive breach. It has also acknowledged that malware was discovered on its payment processing servers at potentially all of its locations beginning at different points in time after March 4, 2019. Wawa claims that based on its investigation, the unauthorized access occurred from March 4, 2019 through December 12, 2019. The information accessed primarily includes payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers.

3. Wawa has acknowledged that it discovered the unauthorized access on December 10, 2019, but has failed to inform the public why it delayed notification of the Data Breach to consumers.

4. The PII for Plaintiff and the class of consumers she seeks to represent was compromised due to Wawa's acts and omissions and their failure to properly protect the PII.

5. Wawa could have prevented this Data Breach. Data breaches at other companies, have occurred.

6. The Data Breach was the inevitable result of Wawa's inadequate approach to data security and the protection of the PII that it collected during the course of its business.

7. Wawa disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and/or payment processor servers and security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

8. As a result of the Wawa Data Breach, the PII of the Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members, or likely to be suffered by Plaintiff and Class members as a direct result of the Wawa Data Breach include:

- a. unauthorized use of their PII;
- b. theft of their personal and financial information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. damages arising from the inability to use their PII;
- e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;
- f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Wawa Data Breach;
- g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already

misused via the sale of Plaintiff and Class members' information on the Internet black market;

h. damages to and diminution in value of their PII entrusted to Wawa for the sole purpose of purchasing products and services from Wawa; and

i. the loss of Plaintiff's and Class members' privacy.

9. The injuries to the Plaintiff and Class members were directly and proximately caused by Wawa's failure to implement or maintain adequate data security measures for PII.

10. Further, Plaintiff retains a significant interest in ensuring that her PII, which, while stolen, remains in the possession of Wawa is protected from further breaches, and seek to remedy the harms she has suffered on behalf of herself and similarly situated consumers whose PII was stolen as a result of the Wawa Data Breach.

11. Plaintiff brings this action to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: statutory damages under state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Wawa to implement improved data security measures.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million exclusive of interest and costs. There are more than 100 putative class members. And, at least some members of the proposed Class have different citizenship from Wawa.

13. This Court has personal jurisdiction over Plaintiff because Plaintiff submits to the Court's jurisdiction.

13. This Court has personal jurisdiction over Defendant pursuant to 18 U.S.C. § 1965(d) because it is found, has agents, and transacts business in this District and because it has its principal place of business in the State of Pennsylvania.

14. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and (c)(2) because Defendant's contacts are sufficient to subject it to personal jurisdiction in this District, and therefore, Defendant resides in this District for purposes of venue, or under 28 U.S.C. § 1391(b)(2) because certain acts giving rise to the claims at issue in this Complaint occurred, among other places, in this District.

PARTIES

15. Plaintiff Ronnie Kaufman is a citizen and resident of the state of Florida. She is a victim of the Data Breach. Ms. Kaufman used her credit card at a Wawa fuel dispenser to purchase gas at the Parkland, Florida location on numerous occasions and has had her credit cards fraudulently compromised on numerous occasions. Plaintiff has spent time and effort monitoring her financial accounts.

16. Defendant Wawa, Inc. is a New Jersey corporation with its principal place of business located at 260 West Baltimore Pike, Wawa, Pennsylvania 19063.

STATEMENT OF FACTS

17. Wawa is an American chain of convenience stores and gas stations located along the East Coast of the United States, operating in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, and Florida. Wawa has more than 750 convenience retail stores with over 500 offering gasoline.

18. According to Wawa's CEO Chris Gheysens open letter to its customers on December 19, 2019, the breach was discovered on December 10, 2019.¹ Wawa's information security team discovered malware on Wawa payment processing servers on December 10, 2019, which it allegedly contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained. The letter states that "[a]t this time, we believe this malware no longer poses a risk to Wawa customers using payment cards at Wawa, and this malware never posed a risk to our ATM cash machines." Malware began running on in-store payment processing systems at potentially all Wawa locations after March 4, 2019. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019.

19. This malware affected payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on December 12, 2019. Most locations were affected as of April 22, 2019.

20. Plaintiff suffered actual injuries in the form of damages to and diminution in the value of her PII – a form of intangible property that Plaintiff entrusted to Wawa and that was compromised in and as a result of the Wawa Data Breach.

21. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

¹ See "An Open Letter from Wawa CEO Chris Gheysens to Our Customers", available at <https://www.wawa.com/alerts/data-security> (last visited December 20, 2019).

22. Moreover, Plaintiff has a continuing interest in ensuring that her private information, which remains in the possession of Wawa, is protected and safeguarded from future breaches.

23. At all relevant times, Wawa was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

24. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Wawa maintained an insufficient and inadequate system to protect the PII of Plaintiff and Class members.

25. PII is a valuable commodity because it contains not only payment card numbers but PII as well. A “cyber blackmarket” exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is “as good as gold” to identity thieves because they can use victims’ personal data to open new financial accounts and take out loans in another person’s name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

26. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant’s data systems; otherwise, they would not aggressively seek or pay for it. For example, in “one of 2013’s largest breaches . . . not only did hackers compromise

the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users.”²

27. At all relevant times, Wawa knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

28. Wawa was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of Wawa’s systems.

29. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Wawa’s approach to maintaining the privacy and security of the PII of Plaintiff and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

30. The ramifications of Wawa’s failure to keep Plaintiff’s and Class members’ data secure are severe.

31. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”³ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.”⁴

32. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have

² Verizon 2014 PCI Compliance Report, available at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter “2014 Verizon Report”), at 54 (last visited December 20, 2019).

³ 17 C.F.R. § 248.201 (2013).

⁴ *Id.*

personal information, “they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance.”⁵

33. Identity thieves can use personal information, such as that of Plaintiff and Class members which Wawa failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver’s license or identification card in the victim’s name but with another’s picture; using the victim’s information to obtain government benefits; or filing a fraudulent tax return using the victim’s information to obtain a fraudulent refund.

34. Javelin Strategy and Research reports that identity thieves have stolen \$112 billion in the past six years.⁶

35. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice’s Bureau of Justice Statistics (“BJS”) found that identity theft victims “reported spending an average of about 7 hours clearing up the issues” and resolving the consequences of fraud in 2014.⁷

36. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

⁵ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited December 20, 2019).

⁶ See <https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point> (last visited December 20, 2019).

⁷ Victims of Identity Theft, 2014 (Sept. 2015) available at: <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited December 20, 2019).

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁸

37. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

38. The PII of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Wawa. Wawa did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

39. The Wawa Data Breach was a direct and proximate result of Wawa's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Wawa's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

40. Wawa had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

⁸ GAO, Report to Congressional Requesters, at 29 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (last visited December 20, 2019).

41. Had Wawa remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Wawa would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

42. As a direct and proximate result of Wawa's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

43. Wawa's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. theft of their personal and financial information;
- b. unauthorized charges on their debit and credit card accounts;

- c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the black market;
- d. the untimely and inadequate notification of the Data Breach;
- e. the improper disclosure of their PII;
- f. loss of privacy;
- g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
- h. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;
- i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;
- j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,
- k. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

44. Wawa has not offered customers any meaningful credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiff and Class members are left to their own actions to protect themselves from the financial damage Wawa has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Wawa's actions have created for Plaintiff and Class members, is ascertainable and is a determination appropriate for the trier of fact. Wawa has also not offered to cover any of the damages sustained by Plaintiff or Class members.

45. While the PII of Plaintiff and members of the Class has been stolen, Wawa continues to hold PII of consumers, including Plaintiff and Class members. Particularly because Wawa has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

46. Plaintiff seeks relief on behalf of herself and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Wawa in December 2019 (**the "Nationwide Class"**).

47. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the laws of the State of Florida, on behalf of a separate Florida State Subclass, defined as follows:

All persons residing in Florida whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Wawa in December 2019 (**the “Florida Subclass”**).

48. Excluded from each of the above Classes are Wawa and any of its affiliates, parents or subsidiaries; all employees of Wawa; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

49. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

50. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

51. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class includes at least millions of individuals whose PII was compromised in the Wawa Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

52. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)’s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

- a. Whether Wawa had a duty to protect PII;

- b. Whether Wawa knew or should have known of the susceptibility of their data security systems to a data breach;
- c. Whether Wawa's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;
- d. Whether Wawa was negligent in failing to implement reasonable and adequate security procedures and practices;
- e. Whether Wawa's failure to implement adequate data security measures allowed the breach to occur;
- f. Whether Wawa's conduct constituted deceptive trade practices under Florida law;
- g. Whether Wawa's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class members;
- h. Whether Plaintiff and Class members were injured and suffered damages or other acceptable losses because of Wawa's failure to reasonably protect its POS systems and data network; and,
- i. Whether Plaintiff and Class members are entitled to relief.

53. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff Kaufman had her PII compromised in the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

54. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Wawa to obtain relief for the Class. Plaintiff has no

conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

55. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Wawa, and thus, individual litigation to redress Wawa's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

56. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

57. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Wawa failed to timely notify the public of the Breach;
- b. Whether Wawa owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Wawa's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;
- d. Whether Wawa failed to adequately comply with industry standards amounting to negligence;
- e. Whether Wawa failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the Class members; and,
- f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

58. Finally, all members of the proposed Class are readily ascertainable. Wawa has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

//

//

//

//

//

COUNT I

NEGLIGENCE

**(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS,
OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)**

59. Plaintiff re-alleges paragraphs 1-58 as if fully set forth herein and further alleges as follows.

60. Upon accepting and storing the PII of Plaintiff and Class Members in its computer systems, networks, and/or payment processor servers, Wawa undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Wawa knew that the PII was private and confidential and should be protected as private and confidential.

61. Wawa owed a duty of care not to subject Plaintiff, along with her PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

62. Wawa owed numerous duties to Plaintiff and to members of the Nationwide Class, including the following:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;
- b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

63. Wawa also breached its duty to Plaintiff and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles,

despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Wawa failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

64. Wawa knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Wawa knew about numerous, well-publicized data breaches.

65. Wawa knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff and Class Members' PII.

66. Wawa breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and/or payment processor servers and data security practices to safeguard PII of Plaintiff and Class Members.

67. Because Wawa knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class members, Wawa had a duty to adequately protect their data systems and the PII contained thereon.

68. Wawa had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Wawa with their PII was predicated on the understanding that Wawa would take adequate security precautions. Moreover, only Wawa had the ability to protect its systems and the PII it stored on them from attack.

69. Wawa's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Wawa's misconduct included failing to: (1) secure its systems, despite

knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

70. Wawa also had independent duties under state and federal laws that required Wawa to reasonably safeguard Plaintiff's and Class members' PII and promptly notify them about the data breach.

71. Wawa breached its duties to Plaintiff and Class members in numerous ways, including:

- a. by failing to provide fair, reasonable, or adequate computer systems and/or payment processor servers and data security practices to safeguard PII of Plaintiff and Class members;
- b. by creating a foreseeable risk of harm through the misconduct previously described;
- c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' PII both before and after learning of the Data Breach;
- d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and
- e. by failing to timely and accurately disclose that Plaintiff's and Class members' PII had been improperly acquired or accessed.

72. Through Wawa's acts and omissions described in this Complaint, including Wawa's failure to provide adequate security and its failure to protect PII of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Wawa

unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff and Class members during the time it was within Wawa possession or control.

73. The law further imposes an affirmative duty on Wawa to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

74. Wawa breached its duty to notify Plaintiff and Class Members of the unauthorized access by failing to provide Plaintiff and Class Members information regarding the breach until December 19, 2019. To date, Wawa has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

75. Through Wawa's acts and omissions described in this Complaint, including Wawa's failure to provide adequate security and its failure to protect PII of Plaintiff and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, Wawa unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff and Class members during the time it was within Wawa's possession or control.

76. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Wawa prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

77. Upon information and belief, Wawa improperly and inadequately safeguarded PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Wawa's failure to take proper security measures to protect sensitive PII of Plaintiff and Class members as described in this Complaint, created

conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiff and Class members.

78. Wawa's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive PII had been compromised.

79. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

80. As a direct and proximate cause of Wawa's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and

the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II

**NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR,
ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)**

81. Plaintiff re-alleges paragraphs 1-58 as if fully set forth herein and further alleges as follows.

82. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wawa, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Wawa’s duty in this regard.

83. Wawa violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Wawa’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Wawa, including, specifically, the immense damages that would result to Plaintiff and Class Members.

84. Wawa’s violation of Section 5 of the FTC Act constitutes negligence per se.

85. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

86. The harm that occurred as a result of the Wawa Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and

avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

87. As a direct and proximate result of Wawa's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III

DECLARATORY JUDGMENT (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA SUBCLASS)

88. Plaintiff re-alleges paragraphs 1-58 as if fully set forth herein and further alleges as follows.

89. As previously alleged, Plaintiff and Class members entered into an implied contract that required Wawa to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Wawa owes duties of care to Plaintiff and Class members that require it to adequately secure PII.

90. Wawa still possesses PII pertaining to Plaintiff and Class members.

91. Wawa has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

92. Accordingly, Wawa has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Wawa's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

93. Actual harm has arisen in the wake of the Wawa Data Breach regarding Wawa's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

94. Plaintiff, therefore, seeks a declaration that (a) Wawa's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Wawa must implement and maintain reasonable security measures, including, but not limited to:

- a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wawa's systems on a periodic basis, and ordering Wawa to promptly correct any problems or issues detected by such third-party security auditors;
- b. engaging third-party security auditors and internal personnel to run automated security monitoring;
- c. auditing, testing, and training its security personnel regarding any new or modified procedures;

- d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Wawa is compromised, hackers cannot gain access to other portions of Wawa systems;
- e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;
- f. conducting regular database scanning and securing checks;
- g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Wawa customers must take to protect themselves.

COUNT IV

VIOLATIONS OF FLORIDA'S UNFAIR TRADE PRACTICES ACT, FLA. STAT. § 501.201, *ET SEQ.* (ON BEHALF OF PLAINTIFF AND THE FLORIDA SUBCLASS)

95. Plaintiff re-alleges paragraphs 1-58 as if fully set forth herein and further alleges as follows.

96. Plaintiff brings this claim for relief individually and on behalf of the Florida Subclass pursuant to Florida's Unfair Trade Practices Act ("FDUPTA"), Fla. Stat. § 501.201, *et seq.*

97. Plaintiff, and members of the Florida Subclass are "persons" within the meaning of FDUPTA.

98. Wawa is engaged in "trade" or "commerce" within the meaning of FDUPTA.

99. FDUPA prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce . . .” § 501.204.

100. As alleged throughout this Complaint, Wawa’s deliberate conduct constitutes deceptive acts or practices in the conduct of business trade or commerce and furnishing of services including:

- a. Failure to maintain adequate computer systems and/or payment processor servers and data security practices to safeguard consumers’ PII;
- b. Failure to disclose that its computer systems and/or payment processor servers and data security practices were inadequate to safeguard consumers’ PII from theft; and
- c. Failure to timely and accurately disclose the data breach to consumer Plaintiff and other members of the classes.
- d. Continued acceptance of PII and storage of other personal information after Wawa knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and
- e. Continued acceptance of PII and storage of other personal information after Wawa knew or should have known of the Data Breach and before it allegedly remediated the Breach.

101. Plaintiff and other members of the classes relied upon Wawa’s deceptive and unlawful conduct.

102. Plaintiff and other members of the classes entrusted Wawa with their PII.

103. Furthermore, as alleged above, Wawa’s failure to secure consumers’ PII violates the FTCA and violates FDUPA.

104. Wawa knew or should have known that its computer systems and/or payment processor servers and data security practices were inadequate to safeguard the PII of Plaintiff and members of the Florida Subclass, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

105. As a direct and proximate result of Wawa's violation of FDUPTA, Plaintiff and members of the Florida Subclass suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and members of the Florida Subclass; damages arising from their inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

106. Wawa's actions and conduct in violating FDUPTA have caused, or are likely to cause substantial damage to Plaintiff and members of the Florida Subclass that includes:

- a. Fraudulent charges on their debit and credit card accounts which may not be reimbursed;
- b. Theft of their PII by criminals;
- c. Costs associated with the detection and prevention of identity theft;
- d. Costs associated with the fraudulent use of their financial accounts;
- e. Loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;
- f. Costs and lost time associated with handling the administrative consequences of the Wawa data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, cancelling and activating payment cards, and shopping for credit monitoring and identity theft protection; and
- g. Impairment to their credit scores and ability to borrow and/or obtain credit; and the continued risk to their PII which remains on Wawa's insufficiently secured systems.

107. As a result of Wawa's deceptive conduct, Plaintiff and members of the Florida Subclass are entitled to relief including restitution of the costs associated with the data breach, disgorgement of all profits accruing to Wawa because of its deceptive acts and practices, attorney's fees and costs, declaratory relief and a permanent injunction enjoining Wawa from its deceptive trade practices.

108. Also, as a direct result of Wawa's knowing violation of FDUPTA, Plaintiff and members of the Florida Subclass are entitled to damages as well as injunctive relief, including, but not limited to:

- a. Ordering that Wawa engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

penetration tests, and audits on Wawa's systems on a periodic basis, and ordering Wawa to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Wawa engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Wawa audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Wawa segment PII by, among other things, creating firewalls and access controls so that if one area of Wawa is compromised, hackers cannot gain access to other portions of Wawa systems;

e. Ordering that Wawa purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Wawa conduct regular database scanning and securing checks;

g. Ordering that Wawa routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Wawa to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Wawa customers must take to protect themselves.

109. Plaintiff brings this action on behalf of herself and members of the Florida Subclass for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and other members of the classes and the public from Wawa's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable

and unlawful practices. Wawa's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

110. Accordingly, Plaintiff and members of the Florida Subclass seek actual damages under Fla. Stat. § 501.211 (2) and all fees, costs, and expenses allowed by law, including attorney's fees and costs, pursuant to Federal Rule of Civil Procedure 23 and Fla. Stat. §§ 501.2105 and 501.211, to be proven at trial.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Wawa as follows:

- a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class, or in the alternative the Florida Subclass;
- b. For equitable relief enjoining Wawa from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;
- c. For equitable relief compelling Wawa to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;
- d. For an award of damages, as allowed by law in an amount to be determined;
- e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;
- f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all issues so triable.

Dated: December 20, 2019

Respectfully Submitted:



Jonathan Shub (PA ID 53965)
Kevin Laukaitis (PA ID 321670)
KOHN, SWIFT & GRAF, P.C.
160 Market Street, Suite 2500
Philadelphia, PA 19103
Phone: (215) 238-1700
jshub@kohnsswift.com
klaukaitis@kohnsswift.com

Melissa R. Emert*
STULL, STULL & BRODY
6 East 45th St. 5th Floor
New York, NY 10017
Phone: (954) 341-5561
memert@ssbny.com

**Pro Hac Vice Application
forthcoming*

*Attorneys for Plaintiff and
the Putative Class*